Docket No. AUS920010952US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Cross**	§	
	§	Group Art Unit: **2136**
Serial No. **10/042,505**	§	
	§	Examiner: **Brandon S. Hoffman**
Filed: **January 9, 2002**	§	
	§	
For: **Secured Radio Communications System, Method, and Computer Program Product**	§	
	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on June 27, 2006.

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

The claims in the application are: 1-7, 9-17, 19-27, 29 and 30.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: None.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-7, 9-17, 19-27, 29 and 30.
4. Claims allowed: None.
5. Claims rejected: 1-7, 9-17, 19-27, 29 and 30.
6. Claims objected to: None.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-7, 9-17, 19-27, 29 and 30.

STATUS OF AMENDMENTS

Applicants filed, together with the notice of appeal, an amendment in response to the final office action of April 12, 2006. The amendment addresses the rejections made under 35 U.S.C. § 112, second paragraph. The Examiner did not enter the amendment.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a method for securing radio transmissions utilizing a conventional radio (Specification, p. 1, ll. 19-22). The method includes the steps of providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 402), said radio including a conventional microphone port that is configured to be coupled to a conventional microphone (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 406) and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 402, 408). The method provides a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 404). The method further includes receiving, within said computer system, an input analog signal from said microphone (Specification, p. 7, ll. 8-20; p. 16, ll. 3-13; and Figure 5, reference numeral 504). The method also includes encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file (Specification, p. 16, ll. 21-30; and Figure 5, reference numeral 510), passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 512), and transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 514).

B. CLAIM 11 - INDEPENDENT

Claim 11 is directed to a system for securing radio transmissions utilizing a conventional radio (Specification, p. 1, ll. 19-22). The system includes a conventional radio, said conventional radio being incapable of encrypting or decrypting signals (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 402), said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified

(Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 406), a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 404), said computer system for receiving an input analog signal from said microphone, said computer system for encrypting said input analog signal utilizing public key encryption to form an encrypted voice file (Specification, p. 16, ll. 21-30; and Figure 5, reference numeral 510), said computer system for passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 512), and said unmodified radio for transmitting said encrypted voice file, wherein radio transmissions from said radio are secured (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 514).

C. CLAIM 21 - INDEPENDENT

Claim 21 is directed to a computer program product executing within a data processing system for securing radio transmissions utilizing a conventional radio, said computer program product on recordable-type media comprising the data processing system implemented steps of an instruction means for providing a conventional radio (Specification, p. 6, ll. 7-15; Specification, p. 1, ll. 19-22). The conventional radio is incapable of encrypting or decrypting signals (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 402), said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 406). The computer program product also includes an instruction means for providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (Specification, p. 13, ll. 9-17; and Figure 4, reference numeral 404), an instruction means for receiving, within said computer system, an input analog signal from said microphone (Specification, p. 16, ll. 21-30; and Figure 5, reference numeral 510), an instruction means for encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 510), an instruction means for passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 512), and an instruction means for transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured (Specification, p. 16, ll. 14-30; and Figure 5, reference numeral 514).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 5, 15 and 25)

Whether claims 5, 15, and 25 are indefinite over for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention under 35 U.S.C. §112, second paragraph.

B. GROUND OF REJECTION 2 (Claims 1-7, 9-17, 19-27, 29, and 30)

Whether the Examiner failed to state a *prima facie* obviousness rejection under 35 U.S.C. § 103(a) against claims 1-7, 9-17, 19-27, 29, and 30 over *Baugh et al.*, Apparatus for Voice Communication Over Local Area Network, U.S. Patent 5,815,553 (September 29, 1998) (hereinafter "*Baugh*") in view of *Herlin et al.*, Method for Secure Communications in a Telecommunications System, U.S. Patent 5,915,021 (June 22, 1999) (hereinafter "*Herlin*"), and further in view of *Ashby et al.*, Apparatus, System and Method for Transmitting Secure Signals Over Narrow Spaced Channels, U.S. Patent 5,305,384 (April 19, 1994) (hereinafter "*Ashby*").

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 5, 15, and 25)

The Examiner rejected claims 5, 15, and 25 as indefinite on the basis that the term "said application" lacks antecedent basis in these claims. In the response to final office action filed on June 27, 2006, Applicants submitted an amendment which would overcome this rejection. Applicants request that the Board of Patent Appeals and Interferences direct that the amendment of June 27, 2006 be entered and that the rejection be overturned on that basis.

B. GROUND OF REJECTION 2

The Examiner rejects claims 1-7, 9-17, 19-27, 29, and 30 as obvious in view of *Baugh*, *Herlin*, and *Ashby*. The Examiner states that:

> Regarding claims 1, 11 and 21, Baugh et al. discloses a method/system/ computer program product for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:
>
> - Providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified (abstract, col. 2, lines 58-62 and fig. 1, ref. num 50, 58, and 62);
> - Receiving, within said computer system, an input analog signal from said microphone (col. 2, lines 58-62);
> - Encrypting, within said computer system, said input analog signal utilizing public key encryption **to form an encrypted voice file** (col. 8**,** lines 44-47); and
> - Passing said encrypted **voice file** from said computer system to said microphone port that is included within said unmodified radio and transmitting said encrypted **voice file** utilizing said unmodified radio, wherein radio transmissions from said radio are secured (col. 3, lines 9-1 4 and fig. 1, ref. num 70 and 74).
>
> Baugh et al. does not specifically teach the input signal is encrypted using public key techniques.
>
> Herlin et al. teaches a method for sending a secure message in a telecommunications system using public key encryption (col. 5, lines 12-35 and col. 9, lines 56-58).

> It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a public key encryption system, as taught by Herlin et al., with the method/system/computer program product of Baugh et al. It would have been obvious for such modifications because the system gains the advantage of securing the recorded message from unauthorized disclosure by an eavesdropper who is monitoring the communication link. By using public key encryption, the recorded message can only be decrypted by the private key that corresponds to the public key used to encrypt the message (see col. 3, lines 60-67 of Herlin et al.).
>
> The combination of Baugh et al. as modified by Herlin et al. do not specifically teach providing a computer system being separate and apart from said radio.
>
> Ashby et al. teaches providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (fig. 1, ref. num 12, separate from the other components).
>
> It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine connecting a radio output to a computer input, as taught by Ashby et al., with the method/system/computer program product of Baugh et al./Herlin et al. It would have been obvious for such modifications because encrypting communications from a radio, who is directly connected to a computing device, prevents eavesdropping on police and military communications by encrypting the data directly from the radio (see abstract and col. 1, lines 18-23 of Ashby et al.).

Final Office Action of April 12, 2006, pp. 3-5 (emphasis in original).

B.1. The Proposed Combination Does Not Teach All of the Features of Claim 1

Claim 1 is a representative claim of the claims in this application. The Examiner has failed to state a *prima facie* obviousness rejection against claim 1 because the proposed combination does not teach or suggest all of the features of claim 1. Claim 1 is as follows:

> 1. A method for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:
>
> providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is

> configured to be coupled to a conventional speaker, said radio remaining unmodified;
>
> providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;
>
> receiving, within said computer system, an input analog signal from said microphone;
>
> encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file;
>
> passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and
>
> transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured.

A *prima facie* case of obviousness is established when the teachings of the prior art itself suggest the claimed subject matter to a person of ordinary skill in the art. *In re Bell*, 991 F.2d 781, 783, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Therefore, the Examiner fails to state a *prima facie* obviousness rejection if the proposed combination does not teach all of the features of the claimed invention. In the case at hand, the teachings of the references when considered as a whole do not teach suggest the claimed subject matter to a person of ordinary skill in the art.

In particular, the combination of references does not teach or suggest the claimed feature of, "providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system" as recited in claim 1. The Examiner asserts otherwise, stating that:

> Ashby et al. teaches providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (fig. 1, ref. num 12, separate from the other components).

Final Office Action of April 12, 2006, pp. 3-5 (emphasis in original).

However, the Examiner's assessment of *Ashby* vis-à-vis claim 1 is incorrect. For example, figure 1 of *Ashby*, cited by the Examiner is as follows:

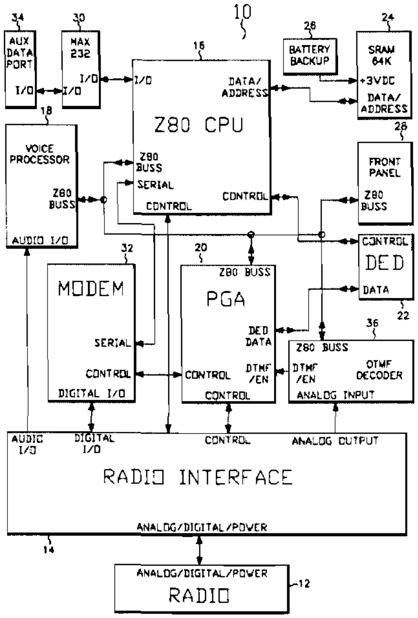

FIG. 1

Figure 1 of *Ashby* shows that radio interface (14) is between the computer (CPU 16) and the radio (12). However, Figure 1 of *Ashby* does not show the microphone, so we turn to Figure 2 of *Ashby* to discern the location of the microphone. Figure 2 of *Ashby* is as follows:

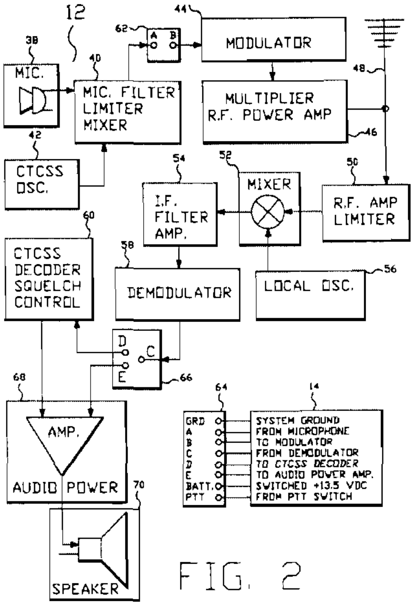

FIG. 2

Figure 2 of *Ashby* is described as, "a block diagram is shown of a conventional analog radio 12 having modifications to accommodate device 10." *Ashby*, col. 19, ll. 64-66. Thus, Figure 2 shows radio 12 in Figure 1. Figure 2 shows microphone (38) as being part of radio (12).

Accordingly, figure 1 and figure 2 together show that the microphone (12) is part of radio (12) in figure 1.

Returning to figure 1, *Ashby* shows that the computer system (16) is not between the microphone (38) and the radio (12). Instead, the microphone (38) is a part of radio (12). For this reason, the computer (16) cannot be between and is not between the microphone (16) and the radio (12). Additionally, *Ashby* never states that the computer system (16) or (10) is between the microphone (38) and the radio (12). Accordingly, *Ashby* does not teach or suggest the claimed feature of, "providing a computer system coupled *between* a microphone and said radio, wherein inputs into said radio are received first by said computer system" as recited in claim 1.

Nevertheless, *Ashby* does show a process of converting an analog voice signal in figure 4. Figure 4 of *Ashby* is as follows:

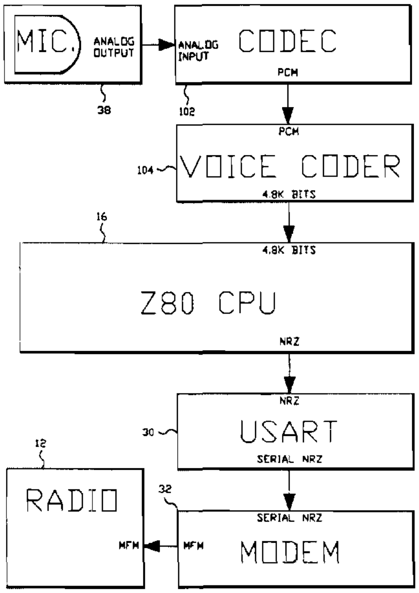

FIG. 4

Ashby describes Figure 4 as follows:

> FIG. 4 is a block diagram illustrating the preferred method of digital voice encoding utilizing device 10 of the present invention. The voice signal begins in analog form at microphone 38. Codec 102 within voice processor block 18 of FIG. 1 converts the analog signal to pulse code modulated (PCM) digital format having a possible serial output of approximately 64,000 BPS. This digital PCM signal is then compressed by the voice coder 104, preferably an STC or IMBE vocoder, which is also contained within a signal processor located with the voice processor block

> Voice coder 104 compresses the serial input producing a possible 4800 BPS of encoded non-return to zero (NRZ) voice data in parallel format which includes appropriate vocoder forward error correction. The 4800 BPS digital voice signal is then sent to CPU 16 where the data is digitally encrypted by DED 22 in 64 bit blocks. Next the critical control information including synchronization, command, digital coded squelch, encryption initialization, end of prologue timer, and control information forward-error correction is added to produce NRZ formatted data output from CPU 16. Various types of control information will be described below and as shown in FIGS. 6, 7 and 8. After the NRZ encrypted signal with unencrypted control information (herein designated "digitally encrypted NRZ signal") is output from CPU 16, it is then passed to USART 30 where the parallel data is converted to serial format. USART 30 then passes the serial digitally encrypted NRZ signal to modem 32 where it is modified (compressed) by a modulation technique suitable for transmission over conventional radio 12. A suitable modulation method is modified frequency modulation (MFM). Modem 32 may advantageously operate at a plurality of operating speeds in response to the command word contained in the control information, or master prologue. The resulting MFM data stream, containing unencrypted control information and modified encrypted digital signals (herein designated "modified digitally encrypted signals") is then sent via tx modem 88 to terminal B of block 62 whereby it is converted to frequency modulated (FM) or phase modulated (PM) as appropriate by modulator 44 and is then transmitted over communication channel 48.

Ashby, col. 21, line 56 through col. 22, line 31.

The cited text describes that the voice digital encoding method as taking place via CPU 16 and radio 12. Thus, the process that takes place in figure 4 is implemented using the devices shown in figure 1.

The process shown in figure 1 provides that the actual analog voice signal is sent from the microphone (38), through the CPU (16) and to the radio (12). Thus, at first glance, one might believe that the CPU (16) is between the radio (38) and the microphone (12). However, figure 4 shows the *process*, not the provision of the actual systems themselves, as recited in claim 1. The provision of the computer system, the microphone, and the radio in *Ashby* is shown in figure 1 which, as shown above, shows the computer system as *not* coupled between the microphone and the radio. Instead, in *Ashby*, the microphone and the radio are directly connected to the computer system. Accordingly, *Ashby* does not teach the claimed feature of, "providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system" as recited in claim 1.

Additionally, *Ashby* does not suggest this claimed feature. As shown above, *Ashby* provides that the microphone and the radio are part of the same component, which is itself connected to the computer system. *Ashby* specifically provides that *Ashby's* system is designed to address the problem of providing encryption/decryption devices which can be retrofitted into existing off-the-shelf conventional radios. *Ashby*, col. 8, ll. 7-9. Conventional off-the shelf radios incorporate the microphone and the radio together, as shown in figure 1 of *Ashby*. For this reason, *Ashby* provides radio interface (14) to interface with the computer system (16). Because *Ashby* specifically provides for interfacing radios and microphones with computer systems and because conventional radios include the microphone with the radio, no reason exists to assume that the computer system should be coupled between a microphone and a radio, as recited in claim 1. Therefore, *Ashby* does not suggest this claimed feature.

Additionally, the Examiner does not assert that either *Baugh* or *Herlin* teach or suggest this claimed feature. The Examiner does not mention *Herlin* in this regard, and the Examiner only asserts *Baugh* to show a radio connected to a microphone and a conventional speaker port.

Additionally, neither *Baugh* nor *Herlin* teach or suggest this claimed feature. *Baugh* is directed to an apparatus for transmitting and receiving voice transmissions over a local area network. *Baugh*, Abstract. *Baugh* is unconcerned with the claimed feature of providing a computer system coupled between a microphone and a radio. Thus, *Baugh* does not teach or suggest the claim feature at issue. In further contrast, *Herlin* is directed to encrypting voice transmissions. *Herlin* is unconcerned with the claimed feature of providing a computer system coupled between a microphone and a radio. Thus, *Herlin* does not teach or suggest the claim feature at issue.

Therefore, none of *Ashby*, *Baugh*, or *Herlin* teach or suggest the claimed feature of, "providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system" as recited in claim 1. For this reason, the proposed combination of *Ashby*, *Baugh*, and *Herlin* when considered together as a whole does not teach or suggest this claimed feature. Accordingly, the Examiner has failed to state a *prima facie* obviousness rejection against claim 1 or against the other claims in this application.

B.2. The Examiner Has Failed to Provide a Proper Teaching, Suggestion, or Motivation to Combine the References

A proper *prima facie* case of obviousness cannot be established by combining the teachings of the prior art absent some teaching, incentive, or suggestion supporting the combination. In re Napier, 55 F.3d 610, 613, 34 U.S.P.Q.2d 1782, 1784 (Fed. Cir. 1995); In re Bond, 910 F.2d 831, 834, 15 U.S.P.Q.2d 1566, 1568 (Fed. Cir. 1990). In the case at hand, the Examiner has failed to establish a teaching, incentive, or suggestion supporting the combination.

Regarding a teaching, suggestion, or motivation to combine the references, the Examiner states that:

> It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a public key encryption system, as taught by Herlin et al., with the method/system/computer program product of Baugh et al. It would have been obvious for such modifications because the system gains the advantage of securing the recorded message from unauthorized disclosure by an eavesdropper who is monitoring the communication link. By using public key encryption, the recorded message can only be decrypted by the private key that corresponds to the public key used to encrypt the message (see col. 3, lines 60-67 of Herlin et al.).
>
> . . .
>
> It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine connecting a radio output to a computer input, as taught by Ashby et al., with the method/system/ computer program product of Baugh et al./Herlin et al. It would have been obvious for such modifications because encrypting communications from a radio, who is directly connected to a computing device, prevents eavesdropping on police and military communications by encrypting the data directly from the radio (see abstract and col. 1, lines 18-23 of Ashby et al.).

Final Office Action of April 12, 2006, pp. 3-5 (emphasis in original).

Thus, the Examiner asserts that it would be obvious to combine *Herlin* and *Baugh* because of the advantage of securing recorded messages. The Examiner also asserts that it would have been obvious to combine *Herlin* and *Baugh* with *Ashby* because encrypting communications from a radio prevents eavesdropping on police and military communications.

However, the Examiner's statements are predicated upon the incorrect assumption that the combination of *Baugh*, *Herlin*, and *Ashby* teach or suggest the claimed feature of, "providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system" as recited in claim 1. As shown above, the proposed combination when considered as a whole does not teach or suggest this claimed feature. Thus, the Examiner's proposed teaching, suggestion, or motivation to combine the references is incomplete. To complete the proposed teaching, suggestion, or motivation, the Examiner would have to also provide a motivation to further modify the combination of *Baugh*, *Herlin*, and *Ashby*. Because the examiner has not done so, the Examiner has failed to state a *prima facie* obviousness rejection against claim 1 or any other claim in this application.

B.3. One of Ordinary Skill Would Not Be Motivated to Combine the References to Achieve the Invention of Claim 1 Because the References Address Different Problems

One of ordinary skill would not combine the references to achieve the invention of claim 1 because the references are directed towards solving different problems. It is necessary to consider the reality of the circumstances--in other words, common sense--in deciding in which fields a person of ordinary skill would reasonably be expected to look for a solution to the problem facing the inventor. *In re Oetiker*, 977 F.2d 1443 (Fed. Cir. 1992); *In re Wood*, 599 F.2d 1032, 1036, 202 U.S.P.Q. 171, 174 (CCPA 1979). In the case at hand, the cited references address distinct problems. Thus, no common sense reason exists to establish that one of ordinary skill would reasonably be expected to look for a solution to the problem facing the inventor. Accordingly, no teaching, suggestion, or motivation exists to combine the references and the Examiner has failed to state a *prima facie* obviousness rejection of claim 1.

For example, *Baugh* is directed to solving the problem of quickly transmitting voice messages over a local area network of computers. For example, *Baugh* provides that:

> Previous systems which provided spoken messages to be transmitted between two computer across a local area network (LAN) were not able to deliver the spoken messages in real-time. Rather, the previous systems operated in a batch mode capacity. These type of voice communication systems recorded an entire spoken message and then play that entire spoken message back at the receiver, although with a substantial time delay between the recording of the message and the playing back.

Baugh, col. 1, ll. 18-26.

On the other hand, *Herlin* is directed to the problem of speeding up secure communications between systems, such as mobile phones, where computational resources for using public key encryption methods are scarce. For example, *Herlin* provides as follows:

> Since the decryption key of each user may be kept totally private, secure methods of communication between users in a telecommunications system that require each user to use and apply his/her decryption key, so that his/her identity can be verified to the other users, would provide good security. However, the use of public key encryption may require intensive use of computational resources in a communicating device such as a mobile phone. The use of public key algorithms to encrypt and decrypt every message or voice communication could be very computationally expensive as compared to private key algorithms.
>
> It would, therefore, be advantageous to provide a method for secure communications between users operating in a telecommunications system, in which public key methods were used to verify the identities of communicating parties, and in which less computationally expensive encryption methods were used once identities are verified.

Herlin, col. 4, ll. 34-51.

In still further contrast, *Ashby* is directed to the problem of retrofitting conventional radios with digital encryption capabilities. For example, *Ashby* provides as follows:

> Thus, a substantial need exists for an encryption/decryption device which can be retrofitted into existing off-the-shelf conventional radios. It also would be advantageous for the device to include re-synchronization capability with the same reliability as the initial synchronization and be capable of inputting into the conventional and trunked radio both control and encrypted voice data within the voice passband of approximately 300-3,200 Hz. Furthermore, if the device can send and receive secure information at varying BPS, the device would not be limited to only one application (i.e., voice or data). It would also be advantageous to provide a control and correction technique that can be designed into or retrofitted into conventional repeaters that controls the repeater functions during digitally encrypted transmissions and error-corrects the critical control information without descrambling the encrypted information. A need also exists for a method and device that can substantially narrow the necessary occupied bandwith below the 15 KHz to 25 KHz spaced channels while being able to use a nonlinear amplifier. Also, a need exists to provide a device which provides forward compatibility of conventional and trunked radios to the new federal standard 1024 and ApCO project 25 digital radio standards in the digital mode.

Ashby, col. 8, ll. 7-31.

Based on the plain disclosures of the references themselves, the references address completely distinct problems that are unrelated to each other. The problem of quickly transmitting voice messages over a local area network of computers is completely distinct from the problem of speeding up secure communications between systems, such as mobile phones, where computational resources for using public key encryption methods are scarce. Similarly, both of these problems are completely distinct from the problem of retrofitting conventional radios with digital encryption capabilities, as described in *Ashby.*

Additionally, the problems and solutions that each reference addresses are so dissimilar from each other that one of ordinary skill *could not* combine the references to achieve the invention of claim 1, even if one of ordinary skill were inspired to so combine the references. In particular, *Baugh* is directed to encrypting voice communications over a local area network, which could possibly be implemented as a wireless radio communication system. *Herlin* is directed to encrypting communications systems between mobile phones and other wireless systems. *Ashby* is directed to providing digital encryption for a conventional radio. Of all these references, only *Ashby* is related to the invention of claim 1. The other references are all completely unrelated to the invention of claim 1 and to *Ashby.* Furthermore, none of the references provide any indication that the methods and devices described in *Herlin* and *Baugh* could be incorporated into the methods and devices described in *Ashby.*

Given the vast difference between implementing communications over a local area network and via a conventional radio, one of ordinary skill could not combine *Ashby* and *Baugh* without more. Given the vast difference between implementing encryption keys in mobile phones to implementing digital encryption with a conventional radio, one of ordinary skill could not combine *Ashby* and *Herlin* without more. Thus, one of ordinary skill would be unable to implement the proposed combination.

Because the references address completely distinct problems, one of ordinary skill would have no reason to combine or otherwise modify the references to achieve the invention of claim 1. Additionally, one of ordinary skill could not combine the references to achieve the invention of claim 1. Thus, no proper teaching, suggestion, or motivation exists to combine the references in the manner suggested by the Examiner. Accordingly, the Examiner has failed to state a *prima facie* obviousness rejection against claim 1 even assuming, *arguendo*, that the Examiner had shown that the combination of references taught all of the features of claim 1 or any other claim in this application.

B.4. One of Ordinary Skill Would Not Be Motivated to Combine the References to Achieve the Invention of Claim 1 Because Each Reference Represents a Complete Solution to the Problem that Each Reference Addresses

As shown above, the Examiner asserts that it would be obvious to combine *Herlin* and *Baugh* because of the advantage of securing recorded messages. The Examiner also asserts that it would have been obvious to combine *Herlin* and *Baugh* with *Ashby* because encrypting communications from a radio prevents eavesdropping on police and military communications. Thus, the Examiner appears to assert that one of ordinary skill would combine all of the references together to achieve the invention of claim 1 because of the advantage of providing security to voice transmissions over a radio.

However, this proposed teaching, suggestion, or motivation is insufficient to serve as a proper teaching, suggestion, or motivation to combine the references to achieve the invention of claim 1 because each reference already accomplishes this goal. For example, *Ashby* already provides a complete solution to the problem of providing digital encryption for conventional radios. *Ashby's* entire disclosure is directed to solving this problem. Moreover, *Baugh* solves the problem of quickly encrypting communications over a local area network. Furthermore, *Herlin* solves the problem of quickly allowing secured communications between systems with limited computing resources. In each case, the problem addressed by the reference is completely solved.

Because each reference provides a complete solution to the problem that each reference represents, one of ordinary skill would have no reason to combine or otherwise modify the references to achieve the invention of claim 1. Accordingly, the Examiner has failed to state a *prima facie* obviousness rejection against claim 1 or any other claim in this application.

B.5. The Age of the References Proves that No Motivation Exists to Combine the References

In addition, the age of the references proves that no motivation exists to combine the references. *Ashby*, the most relevant reference, issued over sixteen years ago in April of 1994. *Baugh* issued nearly eight years ago in September of 1998. *Herlin* issued over seven years ago in June of 1999. Thus, one of ordinary skill has had publicly available the combination of *Ashby*, *Baugh*, and *Herlin* for over seven years.

However, in those intervening seven years no one of ordinary skill has combined the references to achieve the invention of claim 1 because no known publication or product teaches or suggests all of the features of claim 1. In further light of the value of the invention of claim 1, if the invention of claim 1 had been obvious, then one of ordinary skill would have already combined the references and either published a reference describing the claimed invention or produced a product incorporating the claimed invention.

However, the Examiner has been unable to produce a single reference that teaches every feature of claim 1, and Applicants know of no such single reference. In the face of the failure of thousands of computer engineers and software programmers over the last seven years to disclose the invention of claim 1, the natural conclusion to draw is that claim 1 is non-obvious.

Because claim 1 is non-obvious, no teaching, suggestion, or motivation exists to combine the references to achieve the invention of claim 1. Accordingly, the Examiner has failed to state a *prima facie* obviousness rejection against claim 1 or any other claim in this application.

C. CONCLUSION

As shown above, the Examiner has failed to state a *prima facie* obviousness rejection against the grouping of claims represented by claim 1. Therefore, Applicants request that the Board of Patent Appeals and Interferences reverse the rejections of all of the claims. Additionally, Applicants request that the Board direct the Examiner to allow the claims.

/Theodore D. Fay III/
Theodore D. Fay III
Reg. No. 48,504
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal is as follows:

1. A method for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:

providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;

receiving, within said computer system, an input analog signal from said microphone;

encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file;

passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and

transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured.

2. The method according to claim 1, further comprising the step of encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key.

3. The method according to claim 2, further comprising the step of encrypting, within said computer system, said input analog signal utilizing said public key.

4. The method according to claim 1, wherein the receiving step comprises:

receiving, within a first application executing within said computer system, said input analog signal from said microphone;

wherein the encrypting step comprises encrypting, utilizing said first application, said input analog signal utilizing public key encryption to form said encrypted voice file;

wherein the passing step comprises passing said encrypted voice file from said first application to said microphone port of said unmodified radio.

5. The method according to claim 1, wherein the receiving step comprises:

converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format;

constantly monitoring, by a first application, inputs received from said microphone; and

detecting, by said first application, a receipt of said file;

wherein the encryption step comprises in response to a detection by said first application of said receipt of said file, encrypting to form said encrypted voice file, by said first application utilizing a public key that is part of a public key/private key pair assigned to said computer system.

6. The method according to claim 1, further comprising the steps of:

providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified;

providing a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio;

receiving, within said second computer system, an encrypted output from said second speaker port included within said unmodified second radio;

decrypting, within said second computer system, said encrypted output utilizing public key encryption to form a decrypted output; and

outputting said decrypted output from said second computer system to said second speaker.

7. The method according to claim 6, wherein within said second computer system the step of receiving further comprises:

constantly monitoring, by a second application that is executing within said second computer system, said second speaker port;

receiving, by said second application, said encrypted output from said second speaker port;

wherein the decrypting step comprises decrypting, by said second application, said encrypted output utilizing public key encryption.

9. The method according to claim 7, further comprising the steps of:

obtaining, by said second computer system, a private key of said computer system; and

wherein the decrypting step further comprises decrypting said encrypted output utilizing said private key.

10. The method according to claim 9, further comprising the step of exchanging said private key between said computer system and said second computer system prior to transmitting said encrypted voice file.

11. A system for securing radio transmissions utilizing a conventional radio, comprising:

a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;

said computer system for receiving an input analog signal from said microphone;

said computer system for encrypting said input analog signal utilizing public key encryption to form an encrypted voice file;

said computer system for passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and

said unmodified radio for transmitting said encrypted voice file, wherein radio transmissions from said radio are secured.

12. The system according to claim 11, further comprising said computer system for encrypting said input analog signal utilizing a key pair, said key pair including a public key and a private key.

13. The system according to claim 12, further comprising said computer system for encrypting said input analog signal utilizing said public key.

14. The system according to claim 11, said computer system for receiving_further comprising:

a first application executing within said computer system for receiving said input analog signal from said microphone;

said computer system for passing said encrypted further comprises said first application for encrypting said input analog signal utilizing public key encryption to form said encrypted voice file and passing said encrypted voice file from said first application to said microphone port of said unmodified radio.

15. The system according to claim 1 wherein said computer system for receiving comprises:

a microphone driver that is executing within said computer system converting said input analog signal to a file, said file being in a standard voice file format;

a first application constantly monitoring inputs received from said microphone;

said first application detecting a receipt of said file; and

wherein said computer system for encrypting comprises in response to a detection by said first application of said receipt of said file, said first application encrypting said file to form said encrypted voice file by utilizing a public key that is part of a public key/private key pair assigned to said computer system.

16. The system according to claim 11, further comprising:

a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified;

a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio;

said second computer system for receiving an encrypted output from said second speaker port included within said second unmodified radio;

said second computer system for decrypting said encrypted output utilizing public key encryption to form a decrypted output; and

said second computer system for outputting said decrypted output from said second computer system to said second speaker.

17. The system according to claim 16, wherein said second computer system for receiving further comprises:

a second application that is executing within said second computer system constantly monitoring said second speaker port; and

said second application receiving said encrypted output from said second speaker port;

wherein said computer system for decrypting comprises said second application decrypting said encrypted output utilizing public key encryption.

19. The system according to claim 17, further comprising:

said second computer system for obtaining a private key of said computer system; and

wherein said computer system for decrypting further comprises said second computer system for decrypting said encrypted output utilizing said private key.

20. The system according to claim 19, further comprising said computer system for exchanging said private key between said computer system and said second computer system prior to transmissions of radio signals.

21. A computer program product executing within a data processing system for securing radio transmissions utilizing a conventional radio, said computer program product on recordable-type media comprising the data processing system implemented steps of:

instruction means for providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

instruction means for providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;

instruction means for receiving, within said computer system, an input analog signal from said microphone;

instruction means for encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file;

instruction means for passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and

instruction means for transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured.

22. The product according to claim 21, further comprising instruction means for encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key.

23. The product according to claim 22, further comprising instruction means for encrypting, within said computer system, said input analog signal utilizing said public key.

24. The product according to claim 21, wherein the instruction means for receiving are within a first application executing within said computer system, said input analog signal from said microphone;

wherein said instruction means for encrypting utilize public key encryption to form said encrypted voice file;

wherein said instruction means for passing comprises instruction means for passing said encrypted voice file from said first application to said microphone port of said unmodified radio.

25. The product according to claim 21 wherein said instruction means for receiving comprises:

instruction means for converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format;

instruction means for constantly monitoring, by a first application, inputs received from said microphone; and

instruction means for detecting, by said first application, a receipt of said file;

wherein said instruction means for encrypting comprises in response to a detection by said first application of said receipt of said file, instruction means for encrypting, by said first application, said encrypted voice file utilizing a public key that is part of a public key/private key pair assigned to said computer system to form said encrypted voice file.

26. The product according to claim 21, further comprising:

instruction means for providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said radio including a microphone port that is configured to be coupled to a conventional microphone and a speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

instruction means for providing a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio;

instruction means for receiving, within said second computer system, an encrypted output from said second speaker port included within said second unmodified radio;

instruction means for decrypting, within said second computer system, said encrypted output utilizing public key encryption to form a decrypted output; and

instruction means for outputting said decrypted output from said second computer system to said second speaker.

27. The product according to claim 26, wherein said instruction means receiving, within said second computer system further comprises:

instruction means for constantly monitoring, by a second application that is executing within said second computer system, said second speaker port; and

instruction means for receiving, by said second application, said encrypted output from said second speaker port;

wherein said instruction means for decrypting comprises instruction means for decrypting, by said second application, said encrypted output utilizing public key encryption.

29. The product according to claim 27, further comprising:

instruction means for obtaining, by said second computer system, a private key of said computer system; and

wherein said instruction means for decrypting further comprises instruction means for decrypting said encrypted output utilizing said private key.

30. The product according to claim 29, further comprising instruction means for exchanging said private key between said computer system and said second computer system prior to transmitting said encrypted voice file.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.